

What is Future of SOC?

- It is an intelligent, automated, and predictive Cyber Security center.
- It integrates data from multiple sources (networks, cloud, endpoints, users).
- It transforms security from reactive to proactive, with Al-based decisions.

Its main purpose: to reduce detection times, response times, and workload.

Main challenges for SOCs

Hybrid infrastructures that are difficult to protect

High volume of alerts (+333M events / 6 months

Lack of visibility and interoperability between tools

Regulatory pressure (GDPR, NIS2, CRA, etc)

" More than 90% of SOCs still rely on manual processes"



Cyber threat transformation



Intensive use of AI by attackers.



Increase in exploited vulnerabilities



Explosion of attacks with stolen credentials (has multiplied by 5 in 2 years).



Less time to act; from 9 days to less



attacks with stolen

credentials.



of exfiltrations happen in <1 day.

Al integrated Cyber Security evolution

and improve response. False positives have been reduced.

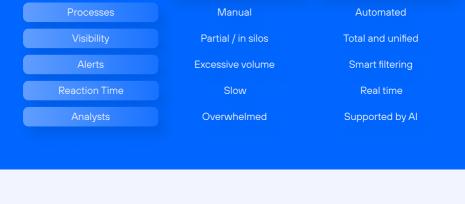
Artificial Intelligence and Machine Learning prioritize threats, reduce alerts,

- Use of LLMs to automate repetitive tasks.
- 20-40% of analyst tasks can be automated

Detection in 10 seconds | Response in 1 minute

of the Future

From Traditional SOC to the SOC



ALL IN REAL TIME,

Modern SOC architecture

